## Understanding GPC Cardholder Fraud

The following guidelines were prepared by the members of the Government Purchase Card (GPC) Joint Fraud Task Force located in Washington, DC.

Fraud is any felonious act of corruption or attempt to cheat the Government or corrupt the Government's agents. GPC cardholders have a responsibility to use the card to procure supplies and services at the direction of the agency under official purchase authorization. Fraudulent purchases include, but are not limited to; 1) purchases which exceed the cardholder's limit; 2) purchases which are not authorized by the agency; 3) purchases for which there is no funding; 4) purchases for personal consumption; 5) purchases which do not comply with Federal Acquisition Regulations; 6) purchases which are billed by the merchant but are never received by the agency; and 7) excessive purchases of necessary items to receive kickbacks, i.e., toners, paper, and other high price items.

Intentional use of the Government Purchase Card for other than official Government business will be considered an attempt to commit fraud against the U.S. Government and will result in immediate cancellation of an individual's purchase card and further disciplinary actions. The cardholder will be held personally liable to the Government for the amount of any non-government transaction. Under 18 U.S.C. 287, misuse of the purchase card could result in a fine of not more than $10,000 or imprisonment for not more than five years or both. Military members that misuse the purchase card may be subject to court martial under 10 U.S.C. 932, UCMJ Art. 132. Depending on the circumstances, other sections of the US Code may apply and may carry additional penalties. An employee found to have misused their card may be subject to personnel actions as provided in the agency regulations.

The purchase card shall be used to purchase supplies and services in accordance with the Federal Acquisition Regulation (FAR). Purchase card use as the procurement and payment tool for micro purchases (less than $2,500) is defined in FAR 13.2. GSA

cardholder training on use of the purchase card may be found at *fss.gsa.gov/webtraining/trainingdocs/smrtpaytraining.cfm*.

For purchases above the micro-purchase threshold, the purchase card may be used as a payment mechanism, not a contracting mechanism. When used as a payment mechanism, contractors may bill against the card. For example, an order has been placed against a GSA Federal Supply Schedule for $15,000. The award was made using the ordering procedures in the Schedule. Instead of issuing an invoice, the contractor agrees to accept payment via purchase card. When the order is delivered, the contractor bills the purchase card account instead of issuing an invoice directly to the agency. All applicable requirements of the Competition in Contracting Act, other statutes and Executive Orders, and the Federal Acquisition Regulations, as well as agency supplements, apply to purchases made with the purchase card as the payment mechanism

**Non-Cardholder Fraud**

Non-cardholder fraud involves use of the card or cardholder data by an unauthorized person. The risk of non-cardholder fraud is higher in certain situations, including:

- **Never received** – a new or replacement card has been mailed to the cardholder but was never received. Due to the possibility that the card could have been intercepted by a third party, the account will be cancelled by the bank upon notification from the cardholder that the card was not received. A new card with a new account number will be issued. Generally cardholders will be required to activate their card by phone once they receive it to ensure that the card has been properly received.
- **Lost card** – The cardholder reports that the card has been misplaced or lost. The account will be closed and a new card issued. Reporting the card as lost does not relieve the Government for payment of any transactions which were made by the cardholder prior to reporting it lost. Cardholders may be required to sign an affidavit confirming their card was lost. If transactions appear on the cardholder statement, which were not made by the cardholder, the cardholder should submit a

dispute form to the bank within 60 days of the disputed statement.

- **Stolen card** – The cardholder reports that the card has been stolen by a third party. The account will be closed and a new card issued. Reporting the card as stolen does not relieve the Government for payment of any transactions which were made by the cardholder prior to reporting it stolen. Cardholders may be required to sign an affidavit confirming their card was stolen. If transactions appearing on the cardholder statement were not made by the cardholder, the cardholder should submit a dispute form to the bank. Failure to submit the dispute form and/or affidavit could result in liability to the Government.

- **Altered or Counterfeit cards** – These types of cards are normally identified by the bank's authorization process or by the cardholder when they receive their statement. Third parties obtained account information and used that information to make purchases with the card. If a fraudulent pattern of use is recognized by the bank at the time of authorization, the bank will validate the use of the card with the cardholder and/or suspend the card. The cardholder may be asked to sign an affidavit verifying that the transactions were fraudulent. If transactions appearing on the cardholder statement were not made by the cardholder, the cardholder should submit a dispute form to the bank. Failure to submit the dispute form and/or affidavit could result in liability to the Government.

- **Account takeover** – This situation may be known as identity theft. In this case the cardholder's identity has been compromised. The third party may request a new card by providing confidential information about the cardholder which they have illegally obtained. Cardholders who may have been subject to identity theft should contact the bank's customer service to prevent the thief from obtaining a card in the cardholder's name.

- **Fraudulent Convenience Check Charges** – This situation may occur when a cardholder's account has been utilized by an unknown entity. Difficulty in verifying this activity occurs often,

because the charges show on the account as cash advances. However, the bank's fraud department is responsible for investigating this matter.

Once it is determined that an account has been compromised, investigation of the activity on the account is the responsibility of the bank. Unless it is determined that a Government employee is involved in the fraud, the agency generally does not participate in the investigation. The account will be closed and a replacement account opened. Non-cardholder fraud is investigated by special units within the banks responsible for initiating civil actions and communicating with Government law enforcement organizations. Any information which you may acquire related to non-cardholder fraud should be reported to your bank. Cardholders should contact customer service at the 800 number provided on the back of the card to report any suspected fraud.

**Indicators of Cardholder Fraud**

- Fraud starts small and may not stop after only one action. No matter how small the misuse, it should be addressed immediately to prevent any future occurrences.

- The card should only be used by the cardholder. If the cardholder is not directly involved in the transaction, there is greater risk that fraud will be committed.

- Cardholders should be able to provide documentation of purchases, i.e., invoices, receipts, etc., when requested by the approving official, A/OPC or auditors.

- Random reviews of cardholder records by the A/OPC will discourage fraud since cardholders and approving officials know someone is watching.

- In many instances. the approving official and/or A/OPC would have detected fraud earlier with proper review.

- Identify the cardholder's duties, what is his/her normal purchase pattern.

*Attachment 1* contains a checklist provided to highlight indicators, which may point to cardholder fraud. It is important to understand that these are indicators only and as such must be investigated further with the cardholder or other individuals as appropriate.

## Types of Reporting Tools Used to Identify GPC Fraud

You can use the GPC's bank electronic access system in order to generate agency reports as a means of detecting fraud. There are several essential reports that can provide transaction data with different levels of detail. Each report can be made available at every level of the hierarchy. The following list of reports may be utilized to detect fraud within your program:

- **Account Activity Report** – This report shows all accounts in the activity and spending for each account during the billing cycle. The report provides details on each transaction such as transaction date, transaction type (credit, debit, convenience check, etc.) merchant name, and dollar amount. This report may be used to sort transactions by dollar size, merchant, date or type. This report is particularly useful for identifying suspicious merchants, unusually high spending patterns, excessive convenience check usage, or untimely purchases.

- **Declined Authorizations** – If available, the declined authorization report will identify cardholders who have attempted to use a card to buy an item for which they are not authorized, which exceeds their single purchase limits, which exceeds their monthly purchase limit or from a merchant which is assigned an inaccurate merchant category code. If a cardholder consistently has declined authorizations, the Program Coordinator should provide additional training or make a change to the cardholder authorization controls or dollar limits to address an official requirement.

- **Disputes** – The disputes report identifies date, merchant, reason code, dollar amount and status of each dispute filed by a cardholder. Reviewing the report would identify cardholders with excessive disputes: cardholder may require training or may be trying to disguise fraudulent activity. Approving officials and Program Coordinator should track and follow-up on disputes to determine the outcome of disputes. Cardholders should attempt to resolve disputes directly with merchants prior to filing a dispute report. If a merchant is consistently appearing on the dispute report, the Program Coordinator should determine whether the merchant has billing issues, quality issues or is attempting to commit fraud by submitting false transactions.

- **Unusual Spending Activity** – The banks offer various reports identifying transactions which may warrant further review. These reports vary by bank.

- **Lost/Stolen Card** – This report identifies cards reported lost or stolen. This report may be reviewed to identify cardholders who have repeatedly reported their cards missing. This may be an indicator that the cardholder needs to secure their card or that the cardholder is attempting to disguise fraudulent activity by denying the charges.

## Schemes From Previous GPC Investigations

The following schemes have been identified during past joint investigations. Obviously there are a host of schemes perpetrated by cardholders and contractors; however, the information listed below is to provide you with an idea of the kinds of schemes perpetrated against the GPC.

1. Vendors continually charged $2499.00 to $2500.00, more than once on the same day, and or every day for one week. It was also identified that on an unspecified date and time the vendors would meet to split profits with cardholder(s).

2. Vendors would conspire with the cardholder to prepare bogus invoices, in which they would prepare phony request orders and then supplement them with phony invoice from the contractor. The cardholder and contractor would then take all proceeds from the transaction.

3. Cardholders would establish front companies to receive payment for merchandise never received. Cardholders would then conspire with either other contractors or other employees to utilize business to obtain larger profit margin and to show some legitimate business is being conducted.

4. Vendors would provide kickbacks to cardholders for their repeated business and loyalty. These kickbacks range from cash payments to gift cards, toys, other items of value.

5. Cardholders and/or approving/billing officials would extort money from vendors by requesting the vendor pay them money for providing their company with continued work.

6. Vendors excessively charge cardholders for low priced items. Vendors would also add unapproved charges to cards.

**Remedies for Contract Fraud**

For every proven case of fraud, there will be a remedy. A remedy is a criminal, civil, contractual or administrative action that should be initiated by a commander or official having responsibility over a matter central to a significant procurement fraud case. This is done in order to protect the interests of the Air Force and to deter future incidents of fraudulent conduct.

Each year, over $40 billion is lost to fraud. As a result, there is a loss of public confidence in our ability to operate efficiently and a loss of buying power for equipment, training, and facilities. It is up to each and every one of us to prevent the needless loss of taxpayer money by preventing fraud, as well as the conditions which lead to it.